DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC REGULATION                                                       17 July 2002
No.    25-73

Information Management

**Hardware Token Use for Public Key Infrastructure**
**Within Army Materiel Command**

**1. Purpose**
This message establishes policy and procedures for the issuance of the Class 3 Release 3 Public Key Infrastructure (PKI) certificates in Army Materiel Command (AMC), AMC Major Subordinate Commands (MSCs), and AMC Separate Reporting Activities (SRAs).

**2. Applicability/scope**
This message is effective immediately and applies to all AMC active Army, Army National Guard and U.S. Army Reserve personnel, AMC civilian employees, and AMC installation-based contractors requiring access to DoD networks.

**3. Background**
   a.  The DoD is implementing the Common Access Card (CAC) to meet the goals of increased efficiency and improved effectiveness within the affected mission areas.  The CAC shall serve as the (1) standard identification card for active-duty military personnel, members of the selected reserve, Army civilian employees, and eligible contractor personnel; (2) principal card used to enable physical access to Army facilities, installations, and controlled spaces; (3) principal card used to enable computer network and system access; and (4) primary PKI token platform for both Class 3 and target Class 4 certificates.

   b.  Headquarters, Army Materiel Command (HQ AMC) is currently assisting the Product Manager Secure Electronic Transaction-Devices (PM SET-D) in deploying PKI certificates throughout the command.  Timing of the PKI deployment is tied to the installation of the Defense Enrollment Eligibility Reporting System (DEERS) and the Real-time Automated

Personnel Identification System (RAPIDS) workstation schedule, and IAW OASD Memo of 12 AUGUST 2000.

**4. Reason for policy**

Some installations will not have DEERS/RAPIDS equipment for CAC issuance in time to meet the October 2003 mandate to digitally sign all Department of Defense (DoD) electronic mail.  To provide PKI capability to those AMC installations that are scheduled late in the DEERS/RAPIDS deployment, or not scheduled at all, AMC will field hardware tokens as an interim solution. AMC has an approved waiver in force to issue DoD Class 3 PKI certificates to AMC personnel that require PKI services prior to the CAC becoming available.  AMC restricts issuance of PKI certificates to hardware tokens because of its enhanced security features.

**5. Policy.**

   a.  For those installations where PKI certificates on a non-CAC medium are to be issued, certificates will be stored on hardware tokens, specifically the Rainbow iKEY 2032 USB, Federal Information Processing Standard (FIPS) 140-1 level 1 or higher.

   b.  Storing PKI certificates on diskettes is only permitted for those installations using Lotus Notes, GroupWise, Eudora, or other non-Microsoft Outlook applications as their email clients.

   c.  All Local Registration Authorities (LRAs) within AMC are required to conduct user registrations and instruct their Trusted Agents (TA) in accordance with this policy.

   d.  Installation DOIMs are required to work in concert with Personnel activities to develop procedures that enable LRAs and TAs to recover hardware tokens from (1) individuals who are out-processing, and (2) individuals who receive their CACs with card readers and middleware. Tokens will be re-initiated for redistribution.

**6. References**

   a.  Memorandum DoD ASD (C3I/CIO), 12 August 2000, Subject: Department of Defense (DoD) Public Key Infrastructure (PKI)

   b.  Message, SAIS-ZA, 14 December 2000, Subject: UNCLAS ALARACT 0109/2000, Interim Policy and Procedures for Public Key Infrastructure (PKI) Implementation in the Department of the Army

   c.  Memorandum, DoD ASD (C3I/CIO) and USD (P&R), 16 January 2001, Subject: Department of Defense (DoD) Common Access Card (CAC)

   d.  Memorandum, Chief of Staff, Army, 18 June 2001, Subject: Army-wide Implementation of the Common Access Card

   e.  Memorandum, Chief of Staff, Army and Secretary of the Army, 8 August 2001, Subject: Army Knowledge Management Guidance Memorandum Number 1

   f.  Memorandum, Dept. of Army, 24 October 2001, Subject: UNCLAS ALARACT 0117/2001, Army-wide Implementation of the DoD Common Access Card (CAC)

g.   Memorandum DoD ASD (C3I/CIO), 21 May 2002, Subject: Public Key Infrastructure (PKI) Policy Update

The proponent of this regulation is the United States Army Materiel Command.  Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to publications and Blank Forms) to Commander, HQ AMC, ATTN: AMCIO-A, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:


OFFICIAL:                                          RICHARD A. HACK
                                                   Major General, USA
                                                   Chief of Staff


LINDA L. PIERPOINT
Chief, IT Programs and Support Division
Office of the Chief Information Officer/G-6

DISTRIBUTION:
Distribution H
Distribution B